

METHOD AND SYSTEM FOR USER AUTHENTICATION IN PORTABLE TYPE DATA COMMUNICATION TERMINAL

Patent number: JP2000003336
 Publication date: 2000-01-07
 Inventor: KATAOKA KENJI
 Applicant: NEC CORP
 Classification:
 - international: G06F15/00; H04Q7/38; H04L9/32
 - european:
 Application number: JP19980167928 19980616
 Priority number(s):

Also published as:

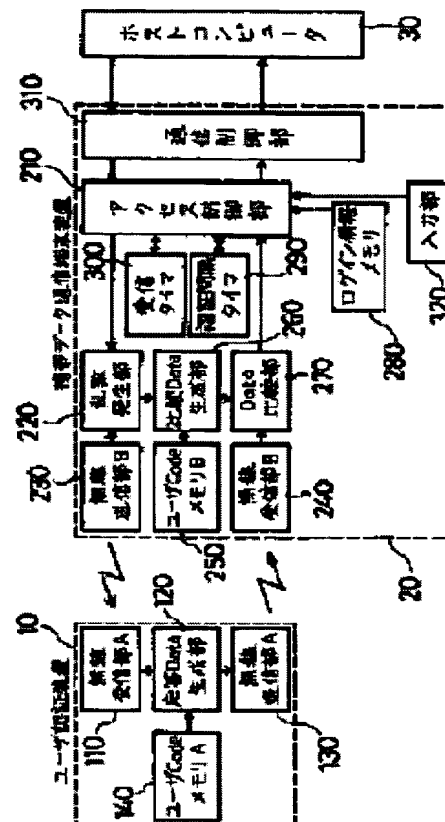


US6515575 (B1)
 GB2341061 (A)

Abstract of JP2000003336

PROBLEM TO BE SOLVED: To provide a user authentication method and a user authentication system which can prevent an illegal use of a portable type data communication terminal by a third party.

SOLUTION: A pair is composed of a user authentication device 10 and a portable type data communication terminal 20 and a memory is made to store a user code common to each other. Then, radio communication is performed by a user log-in demand or timer management at every constant interval of time between these two devices 10 and 20 and it is confirmed that both exist in a communicable distance. Here, if both exist in the communicable distance, it is certified that the portable type data communication terminal 20 is in an appropriate use state and, only when it is certified that it is in this appropriate use state, access to a host computer 30 from the portable type data communication terminal 20 is allowed.



【特許請求の範囲】

【請求項1】 互いに無線通信を行うための無線通信手段を有する携帯型データ通信端末装置とユーザ認証装置とを用いて前記携帯型データ通信端末装置におけるユーザ認証を行うユーザ認証方法であって、

前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにした、

ことを特徴とするユーザ認証方法。

【請求項2】 前記認証情報は、ユーザに固有のコード情報であり、前記携帯型データ通信端末装置の認証情報と、前記ユーザ認証装置の認証情報の一致するか否かを判定することにより、前記認証を行うことを特徴とする請求項1記載のユーザ認証方法。

【請求項3】 前記携帯型データ通信端末装置は、ホスト装置にログイン情報をアクセスすることによって前記ホスト装置にログインする機能を有し、前記認証の結果に応じて、前記ログインを許可するか否かを決定することを特徴とする請求項1記載のユーザ認証方法。

【請求項4】 前記ログイン情報は、前記携帯型データ通信端末装置の記憶手段に予め格納され、前記記憶手段から読み出されて前記ホスト装置に送出されることを特徴とする請求項3記載のユーザ認証方法。

【請求項5】 前記ログイン情報は、ユーザの識別用のアカウント情報と認証用のパスワード情報とからなることを特徴とする請求項3記載のユーザ認証方法。

【請求項6】 前記携帯型データ通信端末装置において特定の動作要求が入力された場合に、前記認証動作を行うことを特徴とする請求項1記載のユーザ認証方法。

【請求項7】 前記認証が一旦が成立した後、一定時間間隔で認証動作を繰り返すことを特徴とする請求項6記載のユーザ認証方法。

【請求項8】 前記認証を行う場合に、携帯型データ通信端末装置からユーザ認証装置に乱数情報を含む認証要求信号を送信し、この認証要求信号を受信したユーザ認証装置で、前記乱数情報とユーザ認証装置が有する認証情報とを含む認証応答信号を生成し、この認証応答信号を携帯型データ通信端末装置に返送し、この認証応答信号を受信した携帯型データ通信端末装置において、前記応答信号から認証情報を抽出し、携帯型データ通信端末装置が有する認証情報と比較することを特徴とする請求項1記載のユーザ認証方法。

【請求項9】 携帯型データ通信端末装置とユーザ認証装置とを備えたユーザ認証システムであって、前記携帯型データ通信端末装置及び前記ユーザ認証装置は、それぞれ自己の認証情報を記憶する記憶手段と、前記認証情報を無線によりやり取りする無線通信手段とを

有し、前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにした、

ことを特徴とするユーザ認証システム。

【請求項10】 前記ユーザ認証装置は、自己の認証情報を前記携帯型データ通信端末装置に無線送信する無線送信手段を有し、

前記携帯型データ通信端末装置は、前記ユーザ認証装置から認証情報を受信する無線受信手段と、受信した認証情報を自己の認証情報と比較する比較手段とを有することを特徴とする請求項9記載のユーザ認証システム。

【請求項11】 前記携帯型データ通信端末装置は、所定の入力に基づいて前記ユーザ認証装置に認証要求を無線送信する無線送信手段を有し、

前記ユーザ認証装置は、前記携帯型データ通信端末装置からの認証要求を受信する無線受信手段を有することを特徴とする請求項10記載のユーザ認証システム。

【請求項12】 前記携帯型データ通信端末装置は、前記認証要求の送信後、前記ユーザ認証装置から一定時間以内に認証情報を受信するか否かを判定する計時手段を有することを特徴とする請求項11記載のユーザ認証システム。

【請求項13】 前記携帯型データ通信端末装置は、ホスト装置にログイン情報をアクセスすることによって前記ホスト装置にログインする機能を有するとともに、前記ログイン情報を予め記憶した記憶手段と、前記記憶手段に記憶したログイン情報を前記ホスト装置に送出するアクセス手段とを有することを特徴とする請求項9記載のユーザ認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯型データ通信端末のユーザ認証方法及びユーザ認証システムに関する。

【0002】

【従来の技術】従来のデータ通信端末装置でホストコンピュータへログインする場合には、ホストコンピュータ側でログインを許可するための情報として、ユーザを識別するためのアカウント名と、ユーザを認証するためのパスワードを使って行われるようになっている。

【0003】図5は、データ通信端末装置をホストコンピュータへログインするための構成例を示すブロック図である。データ通信端末装置20でホストコンピュータ30にログインする場合、ユーザは入力部320から所定の操作によるログイン要求を行う。データ通信端末装置20のアクセス制御部210は、入力部320からのログイン要求があると、通信制御部31を介してホスト

コンピュータ30に接続要求を送出する。

【0004】次に、ホストコンピュータ30よりアカウント名とパスワードを要求されると、アクセス制御部210は、その旨を図示しない表示部によりユーザに通知し、その通知を受けたユーザは、入力部320からログイン情報40であるアカウント名とパスワードを入力する。そして、このログイン情報40がホストコンピュータ30に送られ、パスワードの一致等により、ホストコンピュータ30へのログインが実行される。

【0005】

【発明が解決しようとする課題】しかしながら、上述のような従来の方法では、最近のように携帯型のデータ通信端末装置が普及してくるにつれて、従来の非携帯型装置では自己のオフィス内でのみ行っていたログイン情報の入力を、オフィス以外の場所で行う場合が多くなっていくため、このログイン情報の入力を第3者に盗み見られる危険が大きくなる。また、データ通信端末装置が携帯可能になると、従来の非携帯型装置ではなかったデータ通信端末装置自体の盗難や紛失の可能性も大きくなる。

【0006】そこで本発明の目的は、第3者による携帯型データ通信端末装置の不正使用を防止できるユーザ認証方法及びユーザ認証システムを提供することにある。

【0007】

【課題を解決するための手段】本発明は前記目的を達成するため、互いに無線通信を行うための無線通信手段を有する携帯型データ通信端末装置とユーザ認証装置とを用いて前記携帯型データ通信端末装置におけるユーザ認証を行うユーザ認証方法であって、前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにしたことを特徴とする。

【0008】また本発明は、携帯型データ通信端末装置とユーザ認証装置とを備えたユーザ認証システムであって、前記携帯型データ通信端末装置及び前記ユーザ認証装置は、それぞれ自己の認証情報を記憶する記憶手段と、前記認証情報を無線によりやり取りする無線通信手段とを有し、前記携帯型データ通信端末装置と前記ユーザ認証装置との間で認証情報をやり取りすることにより、前記携帯型データ通信端末装置と前記ユーザ認証装置とが互いに前記無線通信手段の通信可能範囲内に存在することを認証し、前記携帯型データ通信端末装置の所定の動作を許可するようにしたことを特徴とする。

【0009】本発明のユーザ認証方法及びユーザ認証システムにおいて、携帯型データ通信端末装置とユーザ認証装置は2つ1組で構成され、互いに無線通信を行う手段を有する。そして、携帯型データ通信端末装置とユー

ザ認証装置は、それぞれ認証情報を保持しており、この認証情報を携帯型データ通信端末装置とユーザ認証装置との間で無線通信によりやり取りすることで、両者が互いに通信可能範囲内に存在することを認証する。そして、この認証が成功した場合にだけ、携帯型データ通信端末装置の所定の動作、例えばホストコンピュータへのログインを許可する。また、認証が不成功の場合には、携帯型データ通信端末装置がユーザ認証装置より離れた場所で第3者によって不正に使用されている可能性がある」と判断し、携帯型データ通信端末装置の動作を制限する。これにより、携帯型データ通信端末装置の第3者による不正使用を防止できる。

【0010】

【発明の実施の形態】以下、本発明によるユーザ認証方法及びユーザ認証システムの実施の形態について説明する。図1は、本発明によるユーザ認証システムの一例を示すブロック図である。図1に示すように、本例のユーザ認証システムは、ユーザ認証装置10と携帯型データ通信端末装置20とで1つのペアを構成し、これら2つの装置10、20間で、使用者のログイン要求や一定時間毎のタイマ管理によって無線通信を行い、両者が通信可能な距離に存在することを確認することで、携帯型データ通信端末装置20が適正な使用状態にあると認証するものであり、この適正な使用状態にあると認証した場合にだけ、携帯型データ通信端末装置20からのホストコンピュータ30へのアクセスを許可するものである。

【0011】ユーザ認証装置10は、無線受信部A110と、応答Data生成部120と、無線送信部A130と、ユーザCodeメモリ140とを有する。無線受信部A110は、携帯型データ通信端末装置20からの認証要求信号を受信し、認証要求信号の中から乱数Dataを取り出して応答Data生成部120に出力する。ユーザCodeメモリ140は、ユーザ認証装置10が有しているユーザCodeを記憶したものであり、このユーザCodeを応答Data生成部120に出力する。応答Data生成部120は、無線受信部A110より入力された乱数DataとユーザCodeメモリ140より入力されたユーザCodeを用いて、応答Dataを生成し、無線送信部A130に出力する。無線送信部A130は、応答Data生成部120より入力された応答Dataから認証応答信号を生成し、無線信号によって携帯型データ通信端末装置20に送信する。

【0012】一方、携帯型データ通信端末装置20は、アクセス制御部210と、乱数発生部220と、無線送信部B230と、無線受信部B240と、ユーザCodeメモリB250と、比較Data生成部260と、Data比較部270と、ログイン情報メモリ280と、認証間隔タイマ290と、受信タイマ300と、通信制御部310と、入力部320とを有する。アクセス制御部210は、入力部320からのログイン要求に応じて、アクセスするホストコンピュータ30へのログイン・ログアウト

ト処理を制御するものであり、通信制御部310は、ホストコンピュータ30への実際の通信動作を司るものである。乱数発生部220は、アクセス制御部210からの指示により乱数を発生し、無線送信部B230及び比較Data生成部260に対して乱数Dataを出力する。

【0013】無線送信部B230は、乱数発生部220より入力された乱数Dataから認証要求信号を生成し、無線信号によって送信する。無線受信部B240は、ユーザ認証装置10からの認証応答信号を受信し、認証応答信号の中から応答Dataを取り出してData比較部270に出力する。ユーザCodeメモリB250は、ユーザ認証装置10の有するものと同一のユーザCodeを記憶したものであり、比較Data生成部260に対して、ユーザCodeを出力する。

【0014】比較Data生成部260は、乱数発生部220から入力された乱数DataとユーザCodeメモリB250から入力されたユーザCodeとを用いて、比較Dataを生成し、Data比較部270に出力する。Data比較部270は、比較Data生成部260から入力された比較Dataと、無線受信部B240から入力された応答Dataとを比較し、その結果をアクセス制御部210に出力する。受信タイマ300は、アクセス制御部210が乱数発生部220に指示を出した直後からカウントを開始し、一定時間経過しても認証応答信号が受信されなかった場合に、アクセス制御部210へタイムアウトを通知する。ログイン情報メモリ280は、ホストコンピュータ30にログインするために必要な情報がメモリされており、アクセス制御部210からの要求により、ログイン情報を出力する。

【0015】認証間隔タイマ290は、一旦、ログインが認証された後から計時のカウントを開始し、ログイン時と同じ認証通信をユーザ認証装置10に対して一定間隔毎に行うためのタイマであり、タイムアウト時には、その旨をアクセス制御部210へ通知する。この通知に対してアクセス制御部210は、Data比較部270からの比較結果を入力することにより、比較結果が一致なら認証可（以下、認証OKという）として、ログイン情報メモリ280より、ログインに必要な情報を読み出し通信制御部310に出力して、ホストコンピュータ30へのログインを行う。また、比較結果が不一致および受信タイマ300がタイムアウトした場合には、アクセス制御部210は認証不可（以下、認証NGという）として、通信制御部310に対して切断要求を出力し、ホストコンピュータ30との接続を切る。

【0016】以上のように認証間隔タイマ290によって認証動作を行う間隔としては、通信中にユーザ認証装置10を持ったユーザが携帯型データ通信端末装置20から離れた際に他人から使用されないようにすることを考慮した場合には、例えば10秒程度が適当である。ただし、ユーザが席を離れた場合の安全性は、使用するユ

ーザの事情により異なることから、比較的安全性が高い場合には、1分程度であってもよいことが考えられる。また、このような認証時間をユーザが所定の操作を行うことで、認証間隔タイマ290に可変設定できるようにしてもよい。また、ユーザ認証装置10と携帯型データ通信端末装置20との無線通信可能な範囲についても、ユーザの使用環境によって種々考えられるが、例えば数m～十数mの範囲で設定できる。また、例えばユーザ認証装置10における無線送信部A130の送信出力を可変設定可能に構成し、ユーザが適宜選択できるようにしてもよい。

【0017】また、本例において使用するデータ通信の信号フォーマットは、例えば携帯電話（PDC方式）やPHS（パーソナルハンディホンシステム）等の標準規格（RCRSTD-27、28）を用いるものとする。ただし、信号フォーマットとしては、本システムを使用する地域等の通信インフラに依存して、各種のものを採用し得るものである。また、ユーザCodeとしては、長ければ長いほど、セキュリティの面では強固になる。また、本システムでは、番号の重複は許されない。しかしながら、長過ぎても計算等の時間が長くなってしまふ。そこで、一般的には、本例の機能を有する端末が十分普及しても、番号の重複を生じない程度に必要な十分な長さを選択することになる。具体的には、2進数で64桁程度を採用する。また、このようなユーザCodeを格納するメモリA14、メモリB25には、ROMを用いばよい。

【0018】次に、以上のようなシステムにおけるデータ認証方法について図2～図4のフローチャートに従い説明する。図2は、本例におけるユーザ認証装置10の動作を示すフローチャートである。また、図3、図4は、本例における携帯型データ通信端末装置20の動作を示すフローチャートであり、図3は主にアクセス制御部210の動作を示し、図4は、特にユーザ認証装置10と携帯型データ通信端末装置20の間で行う認証通信の動作について示している。

【0019】まず、図2において、ユーザ認証装置10は、電源投入後、通常受信待ちの状態にあって、携帯型データ通信端末装置20からの認証要求信号を待ち受けており、無線受信部A110にて受信ありかどうかをチェックし（ステップS201）、受信がない場合（ステップS202）には、受信信号有無のチェックを繰り返す（ステップS203）。また、受信ありの場合（ステップS204）には、無線受信部A110にて、受信した認証要求信号から乱数Dataを取り出し（ステップS205）、応答Data生成部120へ出力する（ステップS206）。応答Data生成部120は、ユーザCodeメモリA14からユーザCodeを読み出し（ステップS207）、乱数DataとユーザCodeから応答Dataを生成し（ステップS208）、無線送信部A130に出力する（ス

テップS209)。無線送信部A130は、応答Data生成部120から入力された応答Dataより、認証応答信号を生成し(ステップS210)、無線信号にて送信する(ステップS211)。送信後は、再び受信待ち状態に戻る(ステップS203)。

【0020】一方、図3において、携帯型データ通信端末装置20は、電源投入後、通常ログイン要求待ちの状態にあって、入力部320からの入力を待ち受けており、入力部320からのログイン要求があるかどうかをチェックし(ステップS301)、ログイン要求がない場合(ステップS302)には、ログイン要求有無のチェックを繰り返す(ステップS303)。ログイン要求ありの場合(ステップS304)には、認証確認(ステップS400)を行い、ユーザ認証装置10との通信の成否による認証を確認する(ステップS305)。認証確認(ステップS400)の処理については、図4にて説明する。ここで、認証NG(ステップS306)ならば、再びログイン要求待ち状態に戻る(ステップS303)。

【0021】認証OK(ステップS307)ならば、アクセス制御部210は、ログイン情報メモリ280からログイン情報を読み出し(ステップS308)、その情報を通信制御部310へ出力し(ステップS309)、ホストコンピュータ30へログインする(ステップS310)。ログイン後は、アクセス制御部210の指示により、認証間隔タイマ290を開始し(ステップS312)、次の認証確認までのタイムアウト待ち状態となり、タイムアウトをチェックする(ステップS314)。タイムアウトでない場合(ステップS315)は、入力部320からのログアウト要求の有無をチェックし(ステップS317)、ログアウト要求がなければ(ステップS318)、認証間隔タイマ290のタイムアウトチェックへ戻る(ステップS313)。また、ログアウト要求があれば(ステップS319)、認証間隔タイマ290を解除し(ステップS320)、認証NGの場合と同様の処理を行う(ステップS324)。

【0022】また、認証間隔タイマ290がタイムアウトした場合(ステップS316)には、再び認証確認(ステップS400)を行い、ユーザ認証装置との通信の成否による認証を確認する(ステップS321)。ここで、認証OK(ステップS322)ならば、そのまま再度認証確認タイマ29でのループを繰り返す(ステップS311)。認証NG(ステップS323)ならば、アクセス制御部210は、通信制御部310に対して切断要求を出し(ステップS325)、ホストコンピュータ30からログアウトし(ステップS326)、再び入力部320からのログイン要求待ち受け状態に戻る(ステップS303)。

【0023】図4において、認証確認(ステップS400)では、まず、アクセス制御部210からの指示で、

乱数発生部220にて乱数Dataを発生させて無線送信部B230へ出力する(ステップS401)。無線送信部B230は、乱数発生部220から入力された乱数Dataより、認証要求信号を生成し(ステップS402)、無線信号にて送信する(ステップS403)。送信後は、アクセス制御部210の指示により、受信待ち受けのリミット時間である受信タイマ300の計時を開始し(ステップS404)、認証応答信号の待ち受け状態に入る。

【0024】そして、この待ち受け状態中は、無線受信部B240で受信ありかどうかをチェックし(ステップS406)、受信がない場合(ステップS407)には、受信タイマ300のタイムアウトをチェックし(ステップS409)、タイムアウトでなければ(ステップS410)、受信信号有無のチェックを繰り返す(ステップS405)。また、受信ありの場合(ステップS408)には、無線受信部B240は受信した認証応答信号から応答Dataを取り出し(ステップS414)、Data比較部270へ出力する(ステップS415)。また、比較Data生成部260は、乱数発生部220から入力された(ステップS416)乱数Dataと、ユーザCodeメモリB250から読み出した(ステップS417)ユーザCodeを使用して、比較Dataを生成し(ステップS418)、Data比較部270へ出力する(ステップS419)。

【0025】ここで、Data比較部270は、無線受信部B240から入力された応答Dataと、比較Data生成部260から入力された比較Dataとを比較し(ステップS420)、一致していた場合(ステップS422)には、認証OKとし(ステップS423)、不一致だった場合(ステップS421)には、認証NG(ステップS413)とする。そして、認証判定終了後は、受信タイマ300を解除して(ステップS425)、認証確認を終了する(ステップS426)。また、受信タイマ300がタイムアウトした場合(ステップS411)は、比較Dataと応答Dataが不一致の場合と同様の処理(ステップS412)を行う。

【0026】以上のような本例によれば、携帯型データ通信端末装置20において、ユーザ認証装置10と携帯型データ通信端末装置20の両方を揃えないと、ホストコンピュータ30へのアクセスができなくなるため、盗難や紛失による第三者からのホストコンピュータ30に対する不正アクセスのセキュリティを向上することができる。また、本例では、無線通信を利用して非接触で認証を行うため、ユーザ認証装置10と携帯型データ通信端末装置20を別々に持ち歩くことができ、同時に紛失や盗難にあり可能性を少なくすることができる。

【0027】さらに、無線通信で認証を行うため、ユーザ認証装置10と携帯型データ通信端末装置20との距離が離れると認証NGとなり、ユーザ認証装置10を持

ったユーザが一時的に携帯型データ通信端末装置20の側を離れているような場合にも、携帯型データ通信端末装置20によるホストコンピュータ30へのアクセスは阻止でき、セキュリティが保護される。さらに、乱数を利用して毎回認証通信の内容を変更しているため、無線区間での盗聴に対しても保護される。

【0028】また、本例では、認証を行う際に、予めログイン情報メモリ280に記憶したログイン情報を送出することから、その都度ユーザがログイン情報を入力する必要がない。このため、携帯型データ通信端末装置20をオフィス外等で使用して、ホストコンピュータ30にログインする場合にも、ログイン情報を盗み見られることがなくなる効果がある。また、認証に要する時間を短縮でき、また、操作を簡素化することができる効果もある。

【0029】なお、以上の例では、認証の結果により制限する携帯型データ通信端末装置20の動作として、ホストコンピュータ30へのログインを制限する場合について説明したが、他の動作を制限するものであってもよい。

【0030】

【発明の効果】以上説明したように本発明のユーザ認証方法では、携帯型データ通信端末装置とユーザ認証装置との間で無線通信によって認証情報をやり取りすることで、携帯型データ通信端末装置とユーザ認証装置とが互いに無線通信可能な範囲内に存在することを認証し、携帯型データ通信端末装置の所定の動作を許可するようにした。このため、携帯型データ通信端末装置とユーザ認証装置の双方を所有する適正な使用者が携帯型データ通信端末装置を使用する場合にだけ、携帯型データ通信端末装置の動作を許可することができ、携帯型データ通信端末装置の第3者による不正使用を防止できる効果がある。

【0031】また本発明のユーザ認証システムでは、携*

* 帯型データ通信端末装置とユーザ認証装置との間で無線通信によって認証情報をやり取りすることで、携帯型データ通信端末装置とユーザ認証装置とが互いに無線通信可能な範囲内に存在することを認証し、携帯型データ通信端末装置の所定の動作を許可するようにした。このため、携帯型データ通信端末装置とユーザ認証装置の双方を所有する適正な使用者が携帯型データ通信端末装置を使用する場合にだけ、携帯型データ通信端末装置の動作を許可することができ、携帯型データ通信端末装置の第3者による不正使用を防止できる効果がある。

【図面の簡単な説明】

【図1】本発明によるユーザ認証システムの構成例を示すブロック図である。

【図2】図1に示すユーザ認証システムにおけるユーザ認証装置の動作を示すフローチャートである。

【図3】図1に示すユーザ認証システムにおける携帯型データ通信端末装置の動作を示すフローチャートである。

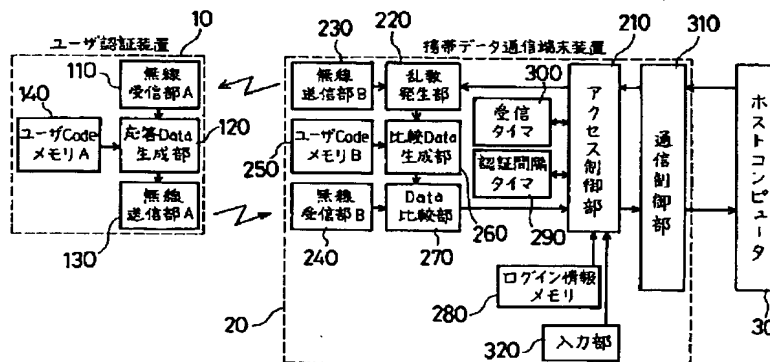
【図4】図1に示すユーザ認証システムにおける認証通信動作を示すフローチャートである。

【図5】従来の携帯型データ通信端末装置とホストコンピュータを用いたシステムの構成例を示すブロック図である。

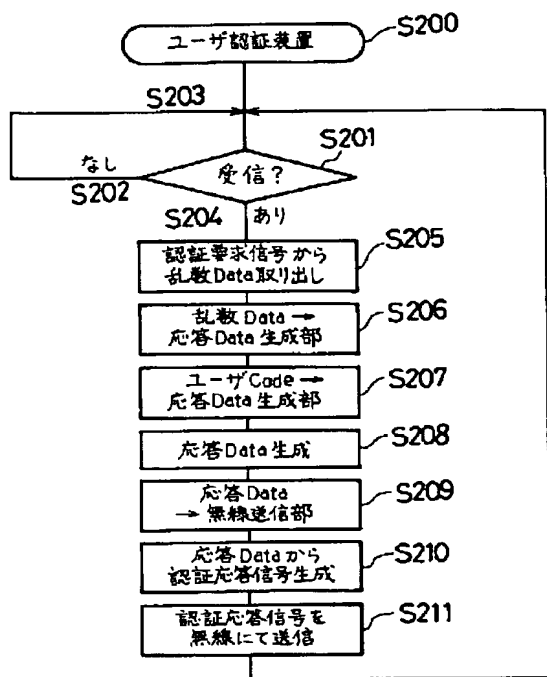
【符号の説明】

10……ユーザ認証装置、20……携帯型データ通信端末装置、30……ホストコンピュータ、110……無線受信部A、120……応答Data生成部、130……無線送信部A、140……ユーザCodeメモリ、210……アクセス制御部、220……乱数発生部、230……無線送信部B、240……無線受信部B、250……ユーザCodeメモリB、260……比較Data生成部、270……Data比較部、280……ログイン情報メモリ、290……認証間隔タイマ、300……受信タイマ、310……通信制御部、320……入力部。

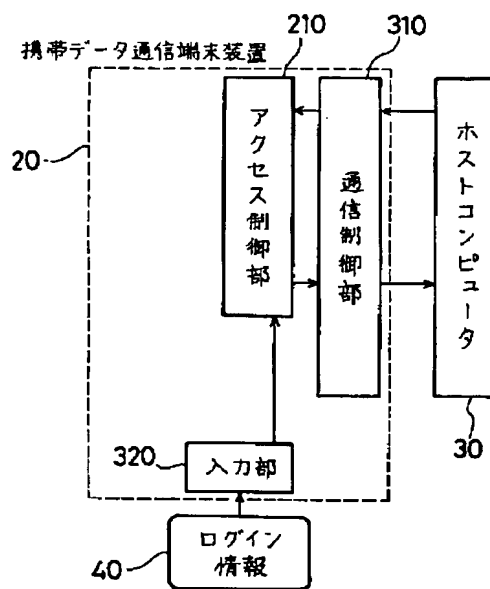
【図1】



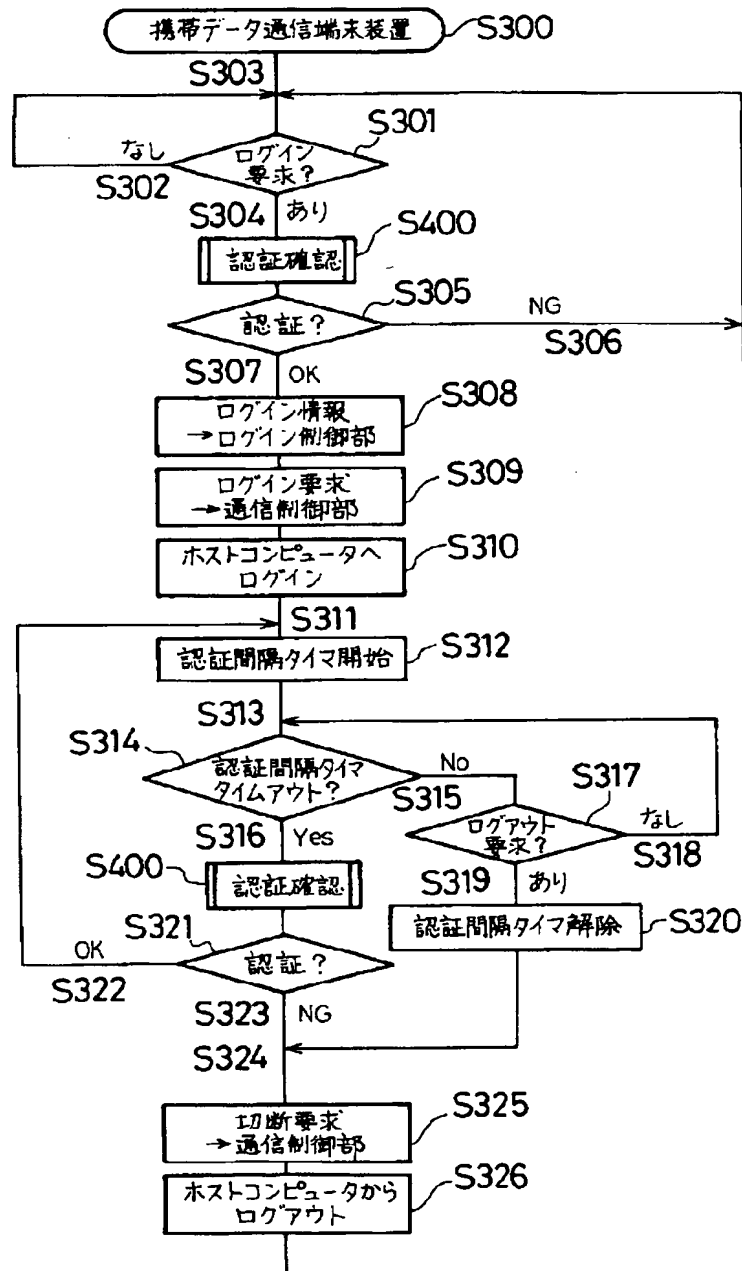
【図2】



【図5】



【図3】



【図4】

